

攻防世界EASYHOOK

原创

[_Outsider_](#) 于 2021-01-11 18:53:33 发布 333 收藏

分类专栏: [攻防世界逆向](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_48274326/article/details/112484344

版权



[攻防世界逆向](#) 专栏收录该内容

18 篇文章 0 订阅

订阅专栏

ida进入主要函数

```
int __cdecl sub_401000(int a1, int a2)
{
    char i; // a1
    char v3; // b1
    char v4; // c1
    int v5; // eax

    for ( i = 0; i < a2; ++i )
    {
        if ( i == 18 )
        {
            *(_BYTE *)(a1 + 18) ^= 0x13u;
        }
        else
        {
            if ( i % 2 )
                v3 = *(_BYTE *)(i + a1) - i;
            else
                v3 = *(_BYTE *)(i + a1 + 2);
            *(_BYTE *)(i + a1) = i ^ v3;
        }
    }
    v4 = 0;
    if ( a2 <= 0 )
        return 1;
    v5 = 0;
    while ( byte_40A030[v5] == *(_BYTE *)(v5 + a1) )
    {
        v5 = ++v4;
        if ( v4 >= a2 )
            return 1;
    }
    return 0;
}
```

找到16进制储存的数据

```
0040A010 2A 50 40 00 00 00 00 00 00 00 00 00 4C 1F 40 00 *P@.....L.~.
0040A020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0040A030 61 6A 79 67 6B 46 6D 2E 7F 5F 7E 2D 53 56 7B 38 ajygfM.._~SV{8
0040A040 6D 4C 6E 00 BB F1 C8 A1 D4 AD 41 50 49 C8 EB BF mLn.获.取.原.API入..
0040A050 DA B5 D8 D6 B7 B3 F6 B4 ED 0A 00 00 57 72 69 74 诒.小.烦.蛆.....Writ
0040A060 5E 4E 50 5C 5E 00 00 00 5D 5E 7D 5E 5E 6C 7D 7D 5E5E k...k...k...
```

按照c程序写个python脚本

```
res=[
    0x61,0x6A, 0x79, 0x67, 0x6B, 0x46, 0x6D, 0x2E, 0x7F, 0x5F, 0x7E,0x2D, 0x53, 0x56, 0x7B, 0x38, 0x6D, 0x4C, 0x
6E, 0x00
]
#奇数时 (input[i]-i)^i
#偶数 (input[i+2])^i
flag=list("1234567891234567890")
for i in range(0,18):
    if i%2==1:
        flag[i]=chr((res[i]^i)+i)
    else:
        flag[i+2]=chr(res[i]^i)
print("".join(flag))
print(res[18]^0x13)

# List() 方法用于将元组转换为列表。
# Python join() 方法用于将序列中的元素以指定的字符连接生成一个新的字符串。
# https://www.runoob.com/python/att-list-list.html
```

得到flag: 1lag{Ho0k_w1th_Fun}